Characterization and Comparison of DDoS Attack Tools and Traffic Generators - A Review

Sunny Behal, Krishan Kumar
(Corresponding author: Sunny Behal)
Department of Computer Science & Engineering, Punjab Technical University
SBS State Technical Campus, Ferozepur, Punjab, India
(Email: sunnybehal@sbsstc.ac.in)
(Received Jan. 13, 2016; revised and accepted Mar. 19 & Apr. 17, 2016)

Abstract

Distributed Denial of Service (DDoS) attack imposes a severe threat to the extensively used Internet based services like e-commerce, e-banking, transportation, medicine, education etc. Hackers compromises the vulnerable systems for launching DDoS attacks in order to degrade or sometimes completely disrupt such services. In recent years, DDoS attacks have been increased in frequency, sophistication and strength. Though a no. of solutions have been proposed in literature to combat against DDoS attacks but still defending from a DDoS attack is a challenging issue. Hackers are also continuously upgrading their skills to launch diversified attacks and are developing new sophisticated attack tools and traffic generators to circumvent these countermeasures. The purpose of this paper is to characterize and compare the popular DDoS attack tools and traffic generators used by the attackers in recent times. The technical details provided would surely help the researchers to handpick the appropriate DDoS attack tool and traffic generator for designing their real experiments so that their proposed DDoS defense methods could be validated in a better way.

Keywords: Attack tools, DDoS, network security, traffic generators

1 Introduction

A DDoS attack is a malicious attempt from multiple systems to make computer or network resources unavailable to its intended users, usually by interrupting or suspending services connected to the Internet [13].

DDoS attacks are launched through the well organized, distributed and remotely controlled network so that compromised computers (called zombies or bots) can be used for sending large volume of continuous and simultaneous attack requests to the target system(s). DDoS attacks mainly cause unusual behavior in the form of unavailability, inability to access the particular website or a service and slow down the performance of the network. As a result, the target systems responds slowly or are completely crashed. The DDoS attacks that are launched by causing the disruption in the legitimate user connectivity (exhaustion of bandwidth, reducing router processing capacity and network resource usage) are termed as Network layer attacks whereas the attacks that are launched by disruption in the legitimate user services (exhaustion of the server resources like CPU, memory, disk/database bandwidth, sockets, input/output bandwidth) are termed as Application layer attacks [1, 6, 7, 12, 15, 29]. In recent years, DDoS attacks have been increased in strength, frequency and sophistication. The attackers are continuously upgrading their skills and modifying their modus operandi and are using latest technologies to launch diversified DDoS attacks. Although, many solutions have been proposed by the researchers to detect, prevent or mitigate DDoS attacks, but still attackers are persistently developing new methods and means to circumvent these countermeasures.

There are number of tools available that can generate the similar looking legitimate traffic as well as attack traffic and can easily circumvent the existing DDoS defense solutions. For example, D-ITG [5, 8, 9, 16, 18] is such a powerful traffic generator that can be used to generate legitimate as well as attack traffic. It has been observed that all of the DDoS attacks are launched now-a-days by using botnets [45].

The key contributions of this paper are:

1) To Identify various attack tools used for launching DDoS attacks.
2) To study and investigate the characteristics of attack tools.
3) To compare and characterize the attack tools on identified attributes.
4) To propose attack tools taxonomy.
5) To identify, compare and characterize various legitimate and background traffic generators.

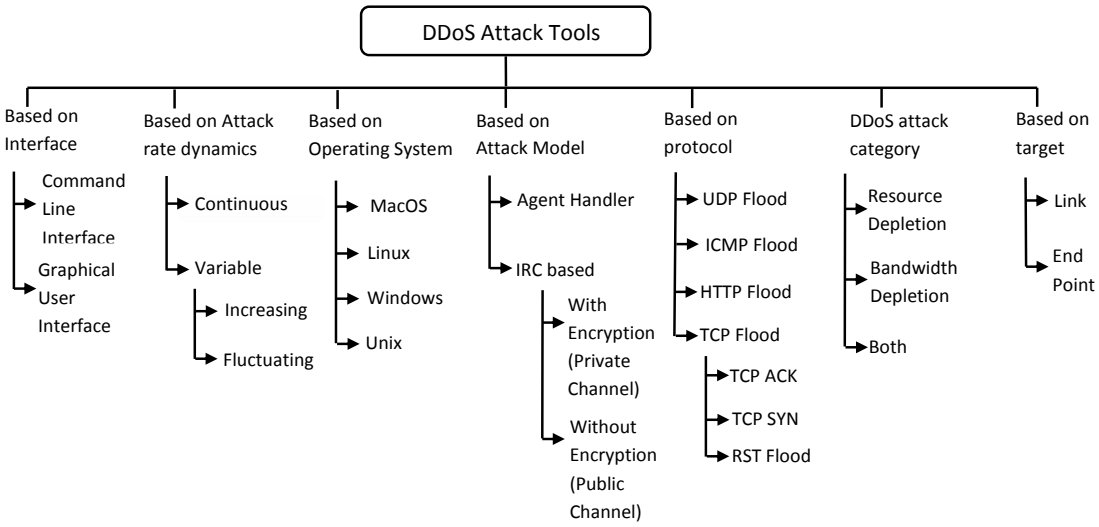

Figure 1: Taxonomy of DDoS attack tools

6) To provide research directions for the design of real-time experiments for validating DDoS defense.

This paper is a unique attempt that highlights the key technical features of the DDoS attack tools and traffic generators used by the attackers to launch DDoS attacks like their architecture model, the type of protocols supported or the type of traffic generated etc. The detailed technical information about the attack tools and traffic generators is provided with reference to the real experimentation purposes so that the internal working of these tools could be unleashed. This information would help the researchers to choose the appropriate DDoS attack tools or traffic generators for their real time experimentations so that better solution to the ever growing DDoS problem could be developed.

In the literature, there are number of existing surveys on the botnets and DDoS attack tools [20, 28, 31, 32, 42, 44] but none of them is complete in itself. Kumar [4], Mirkovic [33] and Specht [41] presented the taxonomies of attack tools but did not categorized the attack tools and traffic generators. Hoque [20] and Srivastva [42] provided the taxonomy of DDoS attacks and key features of few popular DDoS attack tools but lack the technical details. kaur et al. [28] presented the some of the typical DDoS attack tools used by the attackers but did not give any information about traffic generators and their usage. In spite of these extensive surveys, a comprehensive solution to DDoS attacks have not been formulated till date. What is lacking in the literature is the detailed comparison based on the key technical features of the DDoS attack tools and traffic generators so that a better solution could be developed. This survey is first of its kind as per our knowledge that provides the detailed technical details, do the characterization and comparison of popular DDoS attack and traffic generators. There are number of DDoS attack tools and traffic generators available but no one has focused to sum up all the features under single title till date. This paper also provide the detailed comparison of these attack tools and traffic generators along with their technical details.

This paper is organized as follows: Section 2 presents the taxonomy of DDoS attack tools and their description, Section 3 emphasizes on the comparison of the DDoS attack tools based upon their key features, Section 4 provides the comparison of traffic generators and Section 5 concludes the paper by highlighting the need for realtime experimentations.

2 Taxonomy of DDoS Attack Tools and Their Comparison

In this section, the taxonomy of the DDoS attack tools (as shown in Figure-1) is provided based on the identified attributes like type of interface they used, their attack rate dynamics, target operating system, attack model, protocols used, DDoS attack category and target area [4, 21, 27, 33, 41].

Type of Interface used: The interface used by the DDoS attack tools can be either command line interface or graphical user interface. Goldeneye, trinoo, shaft etc. use command line interface whereas hoic, udp flooder, xoic etc use graphical user interface.

Attack rate dynamics: Depending upon the attack rate dynamics, attack tools can either generate the continuous attack traffic (no variations in sending attack request) rate and variable attack rate (tool can vary the attack rate to avoid the detection which can be the increasing rate and fluctuating rate).

Operating System Supported: A number of DDoS attack tools are designed to support the various operating systems like unix, linux, solaris or windows.

Attack model: DDoS attack tools can make use of either Agent-Handler model or and IRC model. Agent-Handler is based on master-slave relation whereas the IRC system use public channels for launching attacks.

Protocol: The type of protocol specifies the kind of traffic generated by the attack tools for generating flood attacks, communication between the agent-handler, handler-client and client-agent. Flood attacks mainly use UDP, ICMP (ICMP ECHO request and ICMP ECHO reply), HTTP, TCP (TCP-SYN, TCP-ACK and RST-flood) protocols.

DDoS attack category: The consequence of a DDoS attack is the unavailability of the resources or bandwidth of the victim. Hence, the attackers use those attack tools that can exhaust target system or network's resources and bandwidth. There are number of DDoS attack tools available that can deplete both the resources and the bandwidth in no time.

Target area: DDoS attacks can either congest the link or end point. So, DDoS attack tools are typically designed for the congestion at the link level(congestion at the victim network) or at the end point level(congestion at the victim server).

All the popular attack tools are compared on the basis of identified key features as shown in Table:1. The key features includes the impact of attack which cause depletion either at bandwidth or resource level, scope of the attack tool, the type of attack launched, support of operating systems, implementation language etc. Further, it has also been observed that all DDoS attack tools follows the same generalized attack tool architecture as given by Lee [41].

Stacheldraht. Stacheldraht is the C-based DDoS tool that can create the ICMP flood, SYN flood, UDP flood and Smurf attack towards the target. It has the capability to congest the link and spoof the IP address. It can run on the Linux and the Solaris 2.1. It has command line based interface and its DDoS attack architecture model is agent based [20].

TFN. TFN (tribe flood network) can generate a number of different kinds of attacks. It is also called the "Son Of Trinoo". It is the command line based which executes on the windows, linux etc. It is written in the C language and has the attack architecture similar to the handler-agent model. It generates DDoS attack that has the capability to deplete both resource and bandwidth [38] of the target.

Trinity. Trinity is the command line based attack tool that can launch UDP, fragment, SYN, RST, random, flags and null flood requests that leads to the endpoint resource exhaustion and link congestion. This tool uses the encrypted format and requires the Linux platform. The architecture model of the Trinity is the IRC-based [20].

Bubonic. A C-based attack tool which can use Linux, Unix and Windows as the underlying platforms for its execution. It is a DoS attempt to exploit or victimize the windows2000 machine by randomly sending a huge volume of the TCP packets with the random settings to increase the load on the machines which leads the machines to a crash. Random settings involve the setting of random IP addresses and random port number [20].

Jolt. A command line based DoS attack tool sends a large number of ICMP packets in order to target the victim machine running on the windows 95 or NT so that the victim machine fails to reassemble them for use. It implementation language is C. However, this kind of attack do not cause any drastic damage to the victim system, and the machine is still in the state, to be recovered [20].

Mstream. A C-based and command line interface DDoS attack tool has ability to forge the source addresses. It creates the TCP ACK flood and TCP RST flood requests to the target server. It can generate botnets and also spoof the ip addresses of the attackers while performing DDoS attacks. Both of these requests can exhaust the network resources and consumes bandwidth of the victim server [38].

Shaft. Shaft is the command line interface DDoS attack tool that can exhaust the bandwidth and resources of the victim server. It provides statistics for TCP, UDP and ICMP flooding attacks and helps the attackers to identify the victim machine status (either completely down or alive) or to decide on the termination of zombies in addition to the attack. Its architecture model is Agent-Handler based [38].

Targa. Targa is the C-based attack tool which can deplete the bandwidth and resources. It is the DoS attack tool which is the collection of the 16 different programs of DoS. These attacks can be launched individually as well as in the group also. It has the ability to spoof the ip addresses and requires the linux platforms [20].

Trinoo. Trinoo is the DDoS attack tool, that uses a master host and several broadcast hosts. Master host instructs the various broadcast hosts to launch the attack. An Application layer attack tool that has the capability to deplete the resources and leverages the bandwidth of the victim network. It is command line based and its architecture model is the Agent-Handler based [38].

Blast20. Blast20 is the DOS attack tool is called as the TCP service stress tool is able to identify the potential weaknesses in the network servers instantly.

Table 1: Comparison of DDoS Attack Tools

Year	Name	Target Impact	Scope	Type of Attack Traffic	Operating System supported	Number of Zombies	whether makes botnets? (yes/no)	Encryption (yes/no)	Ip Spoofing (yes/no)	Implementation Language	Interface Type	Attack Model
1999	Stacheldraht [20]	Bandwidth, Resource	DoS, DDoS	icmp, udp	linux, solaris	Multiple	yes	yes	yes	C	CLI	Agent based
1999	TFN Tribe flood network) [38]	Bandwidth, Resource	DDoS	tcp, udp, icmp	windows, linux,solaris	Multiple	yes	no	yes	C	CLI	Agent based
1999	Trinity cite-Hoq2014	Bandwidth, Resource	DoS, DDoS	tcp, udp	linux	Multiple	yes	no	no	-	CLI	IRC based
2000	Bubonic [20]	Bandwidth, Resource	DoS	tcp	windows, linux, unix	single	no	no	no	C	CLI	-
2000	Jolt [20]	Resource	DoS	icmp	window95, windowsNT	Single	no	no	yes	C	CLI	-
2000	Mstream [38]	Bandwidth	DoS, DDoS	tcp, udp, icmp	linux, windows	Multiple	yes	no	yes	C	CLI	Agent based
2000	Shaft [38]	Bandwidth, Resource	DoS, DDoS	udp,icmp, tcp	linux, unix	Multiple	yes	no	yes	-	CLI	Agent based
2000	Targa [20]	Bandwidth, Resource	DoS	tcp, udp, icmp	linux	Single	yes	no	yes	C	CLI	-
2000	Trinoo [38]	Bandwidth	DDoS	udp, tcp,http	linux, solaris	Multiple	yes	yes	no	C	CLI	Agent based
2001	Blast20 [20]	Resource	DoS	tcp	windows, linux, unix	Single	no	-	-	-	CLI	-
2001	Crazy Pinger [20]	Bandwidth, Resource	DoS	icmp	windows, linux, unix	Single	no	no	yes	-	GUI	-
2001	Kaiten [20]	Bandwidth, Resource	DDoS	tcp, udp	windows	Multiple	Yes	no	no	-	CLI	IRC based
2001	Knight [38]	Bandwidth, Resource	DDoS	tcp, udp	windows	Mutiple	yes	no	-	C	CLI	IRC based
2003	Nemsey [38]	Bandwidth	DoS	tcp	windows	Single	no	no	no	-	GUI	-
2005	FSMax [20]	Resource	DoS	-	windows	Single	no	no	no	-	CLI	-
2005	Hping [20]	Resource	DoS	icmp, udp, tcp	linux, windows	Single	no	no	yes	TCL	CLI	-
2007	Black Energy [20]	Bandwidth, Resource	DDoS	tcp, udp, icmp,http	linux	Multiple	yes	no	-	-	CLI	IRC based
2007	Hgod [20]	Bandwidth, Resource	DDoS	tcp, udp, icmp	windows	Multiple	-	no	yes	-	CLI	IRC based
2007	Panther [20]	Bandwidth	DoS	icmp, udp	-	Single	no	-	-	-	-	-
2007	RefRef [20]	Resource	DDoS	-	windows	Multiple	-	no	no	perl	CLI	IRC based
2008	LOIC [40]	Resource	DoS, DDoS	tcp, udp, icmp,http	linux,mac os,windows,android	Multiple	yes	no	no	C-Sharp	GUI	IRC based
2008	UDP Flooder [40]	Bandwidth	DoS	udp	windows	-	-	no	yes	-	GUI	IRC based
2009	DDOSIM [40]	Resource	DDoS	tcp,smtp,http,udp	linux	Multiple	yes	no	no	C++	CLI	-
2009	Slowloris [40]	Bandwidth, Resource	DoS	http	windows, linux	Single	no	no	no	Perl	GUI and CLI	-
2009	TOR's hammer [38]	Bandwidth, Resource	DoS, DDoS	http	unix, linux, macos	Multiple	yes	no	no	Python	CLI	Agent based
2010	Davoset [38]	Resource	DoS, DDoS	http	linux	Multiple	yes	no	no	Perl	CLI	-
2010	Owasp [37] Http Dos Post	Resource	DoS	http	windows	Single	no	no	no	Python	GUI	-
2010	Pyloris [40]	Resource	DoS, DDoS	tcp,imap, udp,smtp,http, ftp, telnet	linux, windows, macos	Multiple	yes	no	yes	Python	CLI	IRC based
2010	XOIC [40]	Resource	DoS, DDoS	udp, tcp, icmp	windows	Multiple	yes	no	no	C-Sharp	GUI	IRC based
2011	Aldi Botnet [2]	Resource	DDoS	http, tcp	windows	Multiple	yes	no	no	-	GUI	Web based
2011	R-U DEAD -YET [38]	Resource	DoS, DDoS	http	linux	Single	no	no	yes	Python	CLI	-
2011	SSL DoS [25]	Resource	DoS	tcp	windows, unix	Single	no	-	-	-	-	-
2012	Golden-Eye [19]	Resource	DoS	http	Linux, Windows, MAC	Single	no	no	no	Python	CLI	-
2012	HOIC [40]	Resource	DDoS	http	windows	Multiple	yes	no	no	Basic	GUI	-
2012	HULK [38]	Resource	DoS, DDoS	http	linux, windows	Single	no	no	no	Python	CLI	-
-	Silent-Ddoser [3]	Bandwidth, Resource	DDoS	udp, tcp, http	windows	Multiple	yes	yes	no	VB.net	GUI	IRC based
-	SEER [14]	Resource	DDoS	icmp, tcp, udp	windows	Multiple	yes	no	yes	java	GUI	-

It is command line based tool which has the ability to exhaust the resources of the victim server. The parameters required to launch attack are target IP address, start size and end size of the packet [20].

Crazy Pinger. Crazy Pinger is the DoS attack tool which can launch attack by sending a large volume of ICMP packets to the victim machine or to the large remote network. Crazy Pinger is the GUI based attack tool that can spoof the ip addresses and can exhaust the resource and bandwidth. This kind of tool is easy to use and is effective over the multiple platforms [20].

Kaiten. Kaiten is the DDoS attack tool which can launch multiple attacks, viz., UDP flood, TCP flood, SYN flood and PUSH+SYN flood. It uses random source IP addresses for generating botnets. The Kaiten is the command line based tool with IRC as the DDoS attack architecture model. It has the ability to deplete the resource and the bandwidth of the victim server [20].

Knight. Knight is an IRC-based tool can launch multiple DDoS attacks to create SYN flood, UDP flood and urgent pointer flood on windows machines. An IRC based tool that can destroy the resources and the bandwidth of the victim system. It is the command line interface attack tool whose implementation language is the C- language. It can make botnet also [38].

Nemsey. Nemsey is the DoS attack tool whose presence specifies the computer is insecure and infected with the malicious software. It is a GUI based attack tool that can deplete the bandwidth of the victim server. It does not generate the multiple sources and spoof the ip addresses. It attempts to launch an attack with a specified number of packets of specified sizes [38].

FSMax. FSMax is the DoS attack tool which can be used to test the stress of the network and to test the server for buffer overflows which may be exploited during attack, text file is accepted as the input which is executed through a sequence of tests based on the input. FSMax has the ability to exhaust the resources of the victim server [20].

Hping. Hping can handle the random packet size and the fragmentations. Hping performs the firewall rule testing, port scanning and protocol based network performance testing. Its implementation language is TCL and has command line interface [20].

Black Energy. Black Energy is the simple and powerful IRC based architecture model attack tool and a well-known cybercrime toolkit. This tool continues to be widely used to deny services for commercial websites and targets the critical energy infrastructure. It is command line based that can deplete the resources and bandwidth of the victim server [20].

Hgod. Hgod tool is the windows XP based tool which can spoof the source IPs and specifies protocols and the port numbers during the attack. It is used for launching TCP SYN flooding attack. The architecture model is IRC based with command line interface and has the capability to exhaust the resource and bandwidth of the victim server [20].

Panther. A UDP based DoS attack tool that can flood the specified IP at a particular port number. It takes IP address as the input parameter to launch the attack. This tool is the windows based. Panther has the ability to deplete the bandwidth of the victim server and can generate the traffic of UDP and TCP types. However, it is not so powerful attack tool [20].

RefRef. RefRef is the DDoS attack tool which is used to exploit existing SQL injection vulnerabilities. It sends the SQL malformed queries which are carrying payloads that force the servers to exploit their own resources. Its implementation language is PERL and has the command line interface. It is the attack tool that has an architecture model of IRC based model. This tool works with the perl compiler in order to launch DDoS attacks [20].

LOIC. LOIC is an open source network testing tool developed by Praetox Technologies. It was used by 4chan during Project Chanology to attack web servers. It is a GUI based DDoS attack tool which can deplete the resources of the victim server like CPU, memory etc[40].

UDP Flooder. UDP flooder is the port scanner and has the user friendly graphical user interface that can target the random ports and random packet size. It is the IRC-based attack tool which can also spoof the ip addresses of the source. It can deplete the bandwidth of the victim server in no time [40].

DDoSim. A DDoS attack tool that uses the random IP addresses to stimulate several zombies with full TCP connection. DDoSim can generate the HTTP-GET flood attack to target random IP addresses and random ports. A command line interface whose implementation language is the C^{++} and has the ability to deplete the resources of the victim server [40].

Slowloris. Slowloris attack tool creates the flood of TCP SYN requests to the target victim. During the Iranian presidential election in 2009, Slowloris was used as a prominent tool to leverage DoS attacks against sites run by the Iranian government. It has both graphical user and the command line interfaces and is implemented in the perl language [40].

Tor's Hammer. A python based slow post DoS testing tool that runs through TOR network. Tor's Hammer

uses random source IP address making difficult to trace back the source machine of the attacker. This tool that can deplete the bandwidth and resources of the victim server. It has the command line interface and its architectural model is the Agent based model [38].

Davoset. Davoset is a command line tool for conducting DDoS attacks on the sites via Abuse of functionality and XML external entities vulnerabilities at sites for attack on other sites (including DoS and DDoS attacks). Davoset is the PERL based attack tool and has the ability to make the multiple zombies generates the botnets for launching the DDoS attack [38].

Owasp DoS http post. Owasp DoS is the open web application software project for testing performance, availability and capacity planning of web application. Owasp, a graphical user interface is the Slow HTTP POST attack requests are sent to the victim and maintain SSL half connection with the victim. it has ability to deplete the resources of the victim server [37].

Pyloris. Pyloris is the script based tool and is used for testing a service level vulnerability to a particular class of Denial of Service attacks. It uses the inbuilt methods of Slowloris operating system and is used to test the server's readiness to withstand Botnet based DDoS attacks. It is written in Python and has the IRC based attack model [40].

XOIC. Xoic is a GUI based tool that can perform the DDoS attack on any server with specified IP address, a user-selected port and a user-selected protocol. It seems to be more powerful than the Loic. Its implementation language is the C-sharp and has IRC based DDoS attacks that can be performed with TCP, HTTP, UDP, ICMP packet messages [40].

Aldi Botnet. Aldi botnet is a newer inexpensive DDoS bot that is growing in the wild and is designed to deplete the resources of the victim server. Arbor company on September 30,2011 revealed that there are at least 50 distinct aldi botnets that have been seen in the wild with 44 unique command and control points [2].

R-U-dead-Yet. Rudy is the python based slow attack tool to crash the web server. It has two modes, one is the interactive menu mode and another is the unattended configuration based execution mode. A python based tool that can launch attack in order to deplete the resources of the victim server and execute over the Linux platform [38].

SSL DoS. SSl DoS is the windows based tool that can cause denial of service attack without creating the botnets. This tool can be executed on the both windows and Linux, is more effective and powerful. It can launch the network layer flood attacks. It has the ability to exhaust the resources of the victim server [25].

Golden-Eye. Golden-Eye is the multi-threaded python based attack tool that can launch the http flood attack. Attack vector exploitation can be done by HTTP keep alive + no cache messages. It does not encrypt the attack packets and doesn't not support IP spoofing. This tool can execute on the Windows, Linux, MAC operating systems and can deplete the resources of the server [19].

HOIC. High speed, multi-threaded attack tool and has the capability to flood upto 256 websites at once. HTTP GET flood and POST requests are sent to the target server. Anonymous was the first group to utilize it and launch attack against the website of the US department of justice. It has the ability to resource of the victim server [40].

Hulk. HTTP unbearable load king has ability to take down the server in a minute as it directly affects the server's load. It generates TCP SYN flood and multi-threaded HTTP GET flood requests. It can hide the actual user agent. It has the ability to send the different patterns of attack requests that can obfuscate the referrer for each request [38].

Silent ddoser. Silent ddoser can create UDP, SYN and HTTP flood requests to the target victim. It has ability to update the bots on the botnet at ongoing attack. It utilizes triple-DES, RC4 encryption and has IPV6 capabilities with password stealing function. It is a windows tool which has graphical user interface that have the IRC based model [3].

SEER. SEER generates the attack traffic by using the Flooder tool, developed by SPARTA and the Cleo tool developed by UCLA. SEER can generate the same traffic with many variations, can show the movement of traffic from one client to another means the graphical vision of the complete traffic with topology made in the deter testbed. The main disadvantage of this attack tool is, it is only used with the deter testbed. It has graphical user interface and implementation language is java [14].

A wide variety of DDoS attack tools are available on the internet. Most of them are very powerful and destructive; they can easily crash down the target network and web applications in terms of bandwidth and resource depletion in no time. Out of these attack tools Black Energy, Loic, Hoic, r-u-dead-yet and Hulk can generate legitimate looking HTTP traffic. Although Tfn, Trinoo, Stacheldraht, Shaft, Mstream and Trinity have the capabilities to launch powerful DDoS attacks but they are obsolete now a days and are not powerful enough as compared to other attack tools in the list. The parameters required to launch an attack vary with the type of attack

tool used. The year-wise comparison shows the drastic change in the technology wise features of attack tools over the past years.

3 Traffic Generators and Their Comparison

Traffic generators are the tools which can generate the legitimate traffic as well as attack traffic. This section provides the detailed comparison of traffic generators based on their key features as summarized in the Table 2.

Bit-Twist: A highly Scriptable tool which selects the specific range of the packets and then save them in another trace file. It can send multiple trace files at a time and sends the packets at the specific speed. This is Windows and Linux based tool with the feature of the command line computers. It generates the transport layer and the application layer [40].

Byte-Blower: IP testing tool that helps to quickly access the performance and the stability of the IP networks and the network equipment. This gives the real time view. Its implementation language is TCL (tool command language) and is based on the Linux, windows, MacOS [10].

Curl Loader: An Open source and flexible tool for generating and testing of load. Loader uses real HTTP,FTP and TLS/SSL protocol stacks and can simulates tens of thousands and hundreds of users with their own IP addresses. Command line based traffic generator that can run over only linux systems. A tool which can generate the traffic of the application layer and network layer [40].

D-ITG: Distributed internet traffic generator produces traffic that accurately replicates appropriate real time stochastic process by making use of both IDT(inter-departure time) and PS (packet size) features. It is capable of generating traffic at the network, transport and the application layer. It has command line interface which can run on the windows, linux and BSD. The user can generate legitimate traffic, attack traffic and flash traffic [5].

Geist: An internet traffic generator for server architecture evaluation that remains limited to the HTTP GET requests . It can generate the dynamic GET parameters and can also handle the cookies. A command line based traffic generator can generate the traffic of application layer and its implementation language is C. It runs on the windows platform [26].

Harpoon: Harpoon can generate the traffic from traces or from the high- level specification . Harpoon traffic can runs over the HTTP and application behavior that may be different from the real time traffic. A unix based generator which can generate the traffic of application layer, transport layer and the datalink layer. It is used for the testing of network switching hardware [19].

HTTP-Perf: A generator used to measure the web server performance. Its major characteristics includes the robustness (ability to generate and sustains the server overload), support for HTTP/1.1and SSL protocols and extensibility. A command line based traffic generator that can generate application layer traffic with fix number of HTTP GET requests and can be used to check the performance of the web [40].

Iperf: A multi-threaded generator in which client-server can have multiple connections. It is used for active measurements of maximum achievable bandwidth on IP networks. A java based traffic generator which is having graphical user interface as the platform. It can generate network layer and application layer traffic for measuring maximum achievable bandwidth [24].

KUTE: Kernel based traffic engine has KUTE-REC and KUTE-SND. Kute-Rec can count the received packets, inter-arrival time, measures high packet rates and Kute-Snd can generate high packet rate for software solution. A kernel based traffic engine which can generate transport layer traffic and its implementation language is the C [30].

LAN-forge-fire: It is a java based traffic generator with graphical user interface that can generate the application layer traffic against the web-server, VOIP, gateways, firewalls, and load balancers. It requires full TCP connection and provides the support for the hping and nmap [11].

M-GEN: An open source generator that can generates the real time traffic patterns. It can be used in network simulation environment like NS-2 and Opnet. MGEN supports the TCP messaging and the IPv6 networking. A command line based traffic whose implementation languages are TCL and NS-2. It can generate the application layer as well as transport layer traffic [34].

Netperf: An open source generator that can be used to measure the performance of many different types of networks . Its testing is for unidirectional throughput and end-to-end latency. A C-based command line tool which can be executed on the command line based user interface and can generate the transport layer and the network layer traffic [35].

Ostinato: An open source, cross-platform network traffic generator that can craft and send packets of several streams with different protocols at different rates. A python based traffic generator which is having graphical user interface. It can generate the traf-

Table 2: Comparison of traffic generators

Name of Generator	Implementation Language	Type of traffic generated	OS Supported	GUI/CLI	Embedded in Testbed	Input Parameters	Operating Layer	Key Features
SEER [14]	Java	TCP, UDP, HTTP, ICMP	Windows, Linux, Unix	GUI	yes	server IP, client IP, thinking time	Network, Transport, application layer	Legitimate traffic generation, DDoS traffic generation, Visualization
D-ITG [5]	C^{++}	HTTP, TCP/IP	Linux,Windows, Free BSD, OSX(Leopard)	CLI	yes	Inter Departure time, packet size Random and Variable	Transport and application layer	IPv4 traffic generation, IPv6 traffic generation
HTTPerf [40]	-	HTTP, SSL	Linux(Debian), Unix	CLI	no	No. of headers, no. of clients, timeouts, maximum no. of connections	Application Layer	Measures web servers performance, Generates fix no. of HTTP GET requests and keep track on responses by measuring response rate
Pylot [39]	Python	HTTP, HTTPS	Windows XP, Vista, Ubuntu, Cygwin, MACOS	GUI	no	No. of agents, request intervals, rampup time, test duration	Application layer	Multithreaded load generator, Real time stats, Cross platform, Custom timers, Results reports with graphs
Packmime [23]	NS	HTTP	Linux	-	no	response size, request size, flow arrive, server, client, request rate	Transport and Application layers	Simulate different RTT, Bottleneck links, Loss rates
Tmix [17]	NS-2	TCP, IP	Linux	-	Geni Testbed	Load data files,start time	Transport layer	Generate realistic traffic
Ostinato [36]	Python	TCP, ICMP, UDP	Windows,Free BSD, Linux, MACOS	GUI	no	No. of packets, stream rates, no. of streams	Network layer, Transport layer	Cross-platform network traffic generator, Can open,edit,replay,save the pcapfiles
Surge [22]	HTTP	-	-	-	no	-	Application layer	Http traffic generator
Webstone [46]	C	HTTP	WindowsNT, Solaris, UNIX	CLI	Deter testbed	no. of minimum clients, iterations and time per run	Application Layer	Distributed multipurpose benchmark, Measure the performance of the web server's hardware and software products
Geist [26]	C	HTTP	Windows	CLI	no	server, client, protocols	Application Layer	Limited to HTTP GET requests, Does not follow the HTTP redirects
RUDE [40]	C	UDP	Linux	GUI	no	servers, clients, protocols	Transport Layer	Real time UDP data emitter, Generates traffic to the network which can be received and logged on the other site of the network with CRUDE(collector for RUDE)
KUTE [30]	C	UDP	2.6 linux kernel	-	yes	count received packets, inter arrival time, test hardware driver, performance of receiving stack, router/switches	Transport Layer	Kernel based traffic engine
LAN Forge Fire [11]	Java	HTTP, HTTPS,FTP, TELNET, SFTP, TFTP	Linux,Windows, Solaris	GUI	no	Clients, source, packet information	Application Layer	Need full TCP connection, supports many impairments latency, jitter,bandwidth, packet loss, packet reordering
TCP replay [43]	C/C^{++}	TCP, IP	Unix, win32	CLI	Deter testbed	Server, Client, Port No., IP address range	Network Layer	Ability to injects previously captured traffic in libpcap format
MGEN [34]	NS-2, TCL	TCP, UDP, IP	Unix, MACOSX, Win32	CLI	no	Host address, Receive port list, Time to live, type of service, socket buffer size	Network and Transport Layer	TCP Messaging, IPv6 networking, Generates real time traffic patterns, Supports additional statistical patterns, Transport buffering message count, Payload Enhancement
Harpoon [19]	-	HTTP, UDP, TCP, IP	Unix	-	Deter testbed	No. of nodes, file sizes, thinking time, client session, server session, server port	Datalink layer, Transport,Application layer	Generate representative background traffic, Testing of network switching hardware
Bit-Twist [40]	-	TCP, UDP, IP,ARP	Windows, Linux, MACOS X	CLI	no	packet size, request rate	Network and Transport Layer	Powerful libpcap based ethernet packet generator, Complement of TCPDUMP,Capable of sending multiple trace files at a time
Curl Loader [40]	C	HTTP, HTTPS,FTP,FTPS	Linux	CLI	no	Interface, Client, IP address range	Transport and Application Layer	Simulates hundreds of thousands of HTTP/HTTPS and FTP/FTPS clients with its own ip address, FTP Passive and active.
Trafgen [19]	C	HTTP	Linux	CLI	no	Input configuration file,Outgoing traffic devices, no. of frames	Application layer	Fuzzy testing, Fast network traffic generator for debugging and performance evaluation
Netperf [35]	C	TCP, UDP, SCTP, IP	BSD, Unix, Windows, others	CLI	no	minimum interval in real seconds, buffer alignment	Network and Transport Layer	Testing for unidirectional Throughput, Testing for unidirectional end-to-end Latency
Iperf [24]	Java	TCP, UDP, SCTP	Windows, Linux, MACOS, free BSD, openBSD	GUI	no	Specific time, Buffer, target layer bandwidth, protocols	Network and Transport layer	Active measurement of maximum achievable bandwidth on IP network
Byte-Blower [40]	TCL	IP, TCP	Windows, Linux, MACOS	GUI	no	protocols, set latency parameters	Data link,Network, transport layer	IP testing, Scalability of IP network and network impact
Seagull [40]	C^{++}	TCP, UDP, IP, HTTP	Linux, Win32	CLI	no	protocols, user interface Scheduling/core	Network, transport layer and Application layer	Multiprotocol traffic generator, Multithreaded for performance and reliability, Dynamically adjustable scenario rate

fic of network layer and transport layer which is the cross-platform traffic network [36].

Packmime: A HTTP-traffic generator that was developed by the researchers in the internet traffic research group at Bell Labs. Its implementation in NS-2 is done at the UNC-chapelHill. It generates the application layer and transport layer generator. It can simulate different RTT, bottleneck links and loss rates and is publicly available [23].

Pylot: A free open source generator that generates HTTP load tests for the purpose of benchmarking and analysis. It can generate the concurrent load, verifies server responses and produces reports with metrics. A python based graphical user interface tool that is publicly available and generates the application layer traffic. It is a multithreaded load generator [39].

RUDE: Real time UDP data emitter is a flexible programs that can generates traffic and this traffic can be received and logged on the other site of the network with CRUDE(collector of RUDE). A C-based graphical user interface tool that can be used a real time UDP date emitter. It is publicly available and generates the traffic for transport layer [40].

Seagul: An open source tool which allows the additional support of a brand new protocols in less than two hours with no programming knowledge. A powerful traffic generator for functional, load, endurance, stress and performance tests for almost any kind of the protocol. A command line based traffic generator have the C^{++} as its implementation language [40].

SEER: Security experimentation environment(SEER) that developed by SPARTA Inc. It provides the user interface to the experimenters for writing scripts and performs experiments in the Deter environment. A java based traffic generator having the graphical user interface which can generate the legitimate traffic generators [14].

Surge: Scalable URL reference generator that performs reference matching, server file size distribution, request size distribution, relative file popularity, embedded file references. It is the HTTP-based traffic generator which can be used to generate the application layer traffic. It can perform the distribution of the various file [22].

TCP-Replay: It provides the means repeatable and reliable environment for testing a variety of network devices such as switches, routers and firewall networks. It is best suitable for intrusion detection and intrusion prevention systems. A command line based tool which is embedded into the deter testbed and can be used to generate the network layer traffic [43].

Tmix: A traffic generator that is embedded in the GENI platform that is capable of generating the realistic traffic. This generator requires the full TCP and one-way TCP. It can generate the transport layer traffic which is considered as the realistic traffic. It is publicly available over the internet and can execute only on the Linux platform [17].

Trafgen: A multi-threaded network traffic generator with the potential of fuzzy testing that means a packet configuration can be built with random numbers on all or certain packet offsets. It is the C-based traffic generator which is executed by using the command line interface of the linux operating system. It can be used to test the fuzzy system [19].

Webstone: A distributed multi-process benchmark that is embedded in the Deter testbed. It can be used to test the performance of the HTTP in contrast to server's platform. It can measure the average and maximum connect time and the response time. It is the application layer traffic generator which is the CLI based and its implementation language is the C language [46].

A wide variety of traffic generators are available out of which some are licensed and others are free to download. These can be differentiated by using various features like traffic generated type, implementation language, operating system used, layer wise differentiation etc, as summarized in Table 2. The attackers are very smart now a days as they use such traffic generators to generate legitimate looking traffic so as to circumvent the existing defense methods. The need of the hour is to know more and more about the technical details and trends of such attack tools and traffic generators used by the attackers. This information would surely be helpful for the researchers for designing their realtime experiments for the validation of their proposed defense methods.

4 Conclusion

DDoS attack is a severe threat that makes the Internet based web services unavailable to the legitimate users and cause huge financial losses to the communication, banking, medicine and research applications. A number of surveys and taxonomies of DDoS attack tools and traffic generators have been proposed till date but all of them lacks in one dimension or the other. The existing taxonomies have failed to provide the technical details of such tools and their usage. We have done the extensive survey of the popular DDoS attack tools and traffic generators used by the attackers to launch diversity of attacks. In this paper, we have extensively surveyed the popular DDoS attack tools and traffic generators based on the identified key features. Such an extensive survey will surely help the experimenters to hand pick an appropriate attack tool or the traffic generator for designing their real experiments.

Acknowledgments

This Research work has been supported by the All India Council for Technical Education (AICTE), New Delhi, India under Grant Research Promotion Scheme Grant No. 8023/RID/RPS-93/2011-12.

References

[1] M. Aamir and M. A. Zaidi, "DDoS attack and defense: Review of some traditional and current techniques," *CoRR abs/1401.6317*, 2014. (http://docplayer.net/678758-Ddos-attack-and-defense-review-of-some-traditional-and-current-techniques.html)

[2] Aldibotnet, *DDoS Attack Tools*, 2012. (https://asert.arbornetworks.com/ddos-tools)

[3] Arbor Networks, *Silent Ddoser,* 2015. (https://www.arbornetworks.com/blog/asert/tag/silent-ddoser/)

[4] R. Arun and S. Selvakumar, "Distributed denial-of-service (DDoS) threat in collaborative environment - A survey on ddos attack tools and traceback mechanisms," in *Proceedings of IEEE International Conference on Advance Computing*, pp. 1275–1280, 2009.

[5] A. Avallone, A. Pescape and G. Ventre, "Distributed Internet Traffic Generator (D-ITG): Analysis and experimentation over heterogeneous networks," in *International Conference on Network Protocols*, Atlanta, Georgia, 2003.

[6] S. Behal, A. S. Brar, and K. Kumar, "Signature-based botnet detection and prevention," in *Proceedings of International Symposium on Computer Engineering and Technology*, pp. 127–132, 2010.

[7] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita, "Detecting distributed denial of service attacks: methods, tools and future directions," *The Computer Journal*, vol. 57. no. 4, pp. 537–556, 2013.

[8] A. Botta, A. Dainotti, and A. Pescape, "A tool for the generation of realistic network workload for emerging networking scenarios," *Elsevier Journal of Computer Networks*, vol. 56, no. 15, pp. 3531–3547, 2012.

[9] V. Bukac, *Traffic Characteristics of Common DoS Tools*, Technical Report FIMU-RS-2014-02, 2014.

[10] ByteBlower, *ByteBlower*, 2014. (https://www.excentis.com/blog/)

[11] Candela Technologies, *Lanforge Fire: Network Testing and Emulation Solutions*, 2015. (http://www.candelatech.com)

[12] G. Carl, G. Kesidis, R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet Computing*, vol. 10, no. 1, pp. 82–89, 2006.

[13] CERT, *Computer Emergency Report Team (CERT)*, 2015. (http://www.cert.org/)

[14] DeterLab, *SEER: The Security Experimentation EnviRonment*, 2012. (http://seer.deterlab.net/trac)

[15] D. Dittrich, *The DoS Project's Trinoo, Distributed Denial of Service Attack Tool*, 1999. (http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt)

[16] C. Douligeris and A. Mitrokotsa, "Ddos attacks and defense mechanisms: classification and state-of-the-art," *Elsevier Journal of Computer Networks*, vol. 44, no. 5, pp. 643–666, 2004.

[17] Geni, *Tmix*, 2011. (http://groups.geni.net/geni/wiki/genitmix)

[18] S. Ghansela, "Network security: Attacks, tools and techniques," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 6, pp. 419–421, 2013.

[19] Github, *DDoS Attack Tools*, 2013. (https://github.com/)

[20] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya, and J. K. Kalita, "Network attacks: Taxonomy, tools and systems," *International Journal of Network and Computer Applications*, vol. 40, pp. 307–324, 2014.

[21] A. Hussain, S. Schwab, S. Fahmy, J. Mirkovic, R. Thomas, "DDoS Experiment methodology," in *Proceedings of DETER Community Workshop on Cyber Security Experimentation*, pp. 8–14, 2006.

[22] ICIR, *Traffic Generators for Internet Traffic*, 2010. (http://www.icir.org/models/trafficgenerators.html)

[23] Internet Traffic Research Group, *Packmime*, 2005. (http://www.isi.edu/nsnam/ns/doc/node555.html)

[24] iPerf, *iPerf - The Network Bandwidth Measurement Tool*, 2015. (https://iperf.fr/iperf-download.php)

[25] Kali Linux Tutorials, *THC-SSL-DoS - A Denial of Service Tool Against Secure Web-servers and for Testing SSL-Renegotiation*, 2011. (https://www.thc.org/thc-ssl-dos)

[26] K. Kant, V. Tewari, and R. Iyer, "Geist: A web traffic generation tool," in *Proceedings of International Conference on Modelling Techniques and Tools for Computer Performance Evaluation*, pp. 227–232, Springer, 2002.

[27] A. Kapravelos, C. Grier, N. Chachra, C. Kruegel, G. Vigna, and V. Paxson, "Hulk: Eliciting malicious behavior in browser extensions," in *Proceedings of 23rd USENIX Security Symposium*, pp. 641–654, 2014.

[28] H. Kaur, S. Behal, and K. Kumar, "Characterization and comparison of distributed denial of service attack tools," in *Proceedings of IEEE International Conference on Green Computing and Internet of Things (ICGCIoT'15)*, pp. 1139–1145, 2015.

[29] N. Kaur and S. Behal, "P2P-BDS: Peer-2-Peer botnet detection system", *IOSR Journal of Computer Engineering*, vol. 16, no. 5, pp. 28–33, 2014.

[30] Kute, *KUTE – Kernel-based Traffic Engine*, 2007. (http://caia.swin.edu.au/genius/tools/kute/)
[31] C. Liu, C. Peng, and I. Lin, "A survey of botnet architecture and batnet detection techniques," *International Journal Network Security*, vol. 16, no. 2, pp. 81–89, 2014.
[32] M. Mahmoud, M. Nir, and A. Matrawy, "A survey on botnet architectures, detection and defences.," *International Journal Network Security*, vol. 17, no. 3, pp. 264–281, 2015.
[33] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *International Journal ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.
[34] U.S. Naval Research Lab, *Networks & Communications Systems Downloads*, 2015. (http://downloads.pf.itd.nrl.navy.mil/mgen)
[35] Netperf, *Netperf Homepage*, 2015. (http://www.netperf.org/netperf)
[36] Ostinato, *Network Traffic Generator and Analyzer*, 2010. (http://ostinato.org/)
[37] OWASP, *Open Web Application Security Project*, 2014. (https://www.owasp.org/)
[38] Packet Storm, *DDoS Attack Tools*, 2015. (http://packetstormsecurity.org)
[39] Pylot, *Pylot - Web Performance Tool*, 2007. (http://www.pylot.org/)
[40] Sourceforge, *DDoS Attack Tools*, 2012. (http://sourceforge.net/projects)
[41] S. M. Specht and R. Lee, *Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures*, pp. 543–550, ISCA PDCS, 2004.
[42] A. Srivastava, B. B. Gupta, A. Tyagi, A. Sharma, and A. Mishra, "A recent survey on ddos attacks and defense mechanisms," in *Advances in Parallel Distributed Computing*, pp. 570–580, Springer, 2011.
[43] Tcpreplay, *Tcpreplay*, 2014. (http://tcpreplay.synfin.net)
[44] M. Uma and G. Padmavathi, "A survey on various cyber attacks and their classification.," *International Journal Network Security*, vol. 15, no. 5, pp. 390–396, 2013.
[45] F. Wang, H. Wang, X. Wang, and J. Su, "A new multistage approach to detect subtle ddos attacks," *Joournal of Mathematical and Computer Modelling*, vol. 55, no. 1, pp. 198–213, 2012.
[46] WebStone, *The Benchmark for Web Servers*, 2002. (http://www.mindcraft.com/webstone/)

Biography

Sunny Behal has done Bachelor of Technology in Computer Science and Engineering from SBS State Technical Campus, Ferozepur, Punjab, India in 2002. He finished his Masters in Computer Science and Engineering from Guru Nanak Dev Engineering College, Ludhiana, Punjab, India in 2010. His Research interests includes Botnets, DDoS attacks, Information and Network Security. Currently, He is full time Ph.D. Research Scholar at SBS State Technical Campus, Ferozepur and have published more than 40 Research papers in different International Journals and Conferences of repute.

Krishan Kumar has done Bachelor of Technology in Computer Science and Engineering from National Institute of Technology, Hamirpur in 1995. He finished his Masters in Software Systems from BITS Pilani in 2001. He finished his Ph. D. from Department of Electronics and Computer Engineering at Indian Institute of Technology, Roorkee in 2008. Currently, he is working as Associate Professor at SBS State Technical Campus, Ferozepur, Punjab, India. His general research Interests are in the areas of Information Security and Computer Networks. He has published around 200 + research papers in different International Journals and Conferences of Repute including more than 500 citations.